Induction and Loops

SFWR ENG 2FA3

Ryszard Janicki

Department of Computing and Software, McMaster University, Hamilton, Ontario, Canada

Introduction

The set $\mathbb{N}$ of natural numbers $\{0, 1, 2, \cdots\}$ is infinite

- How to prove properties of such an infinite set?
- It requires a technique that is of fundamental importance in mathematics and computer science: mathematical induction
- We investigate
  1. Mathematical induction
  2. Induction over sets other than $\mathbb{N}$
- We show how properties of an inductively defined function can be proved using induction
- We show how a program loop can be analysed using induction

Induction over the natural numbers

Claim

$$P(n): \quad +(i \mid 1 \le i \le n : 2i - 1) = n^2$$

- *$P(n)$ is a boolean expression*
- *We can view it as a boolean function $P(n : \mathbb{N})$ of its free variable n*

Example

$1 + 3 = (2 \cdot 1 - 1) + (2 \cdot 2 - 1) = 2^2$

Example

$1 + 3 + 5 = (2 \cdot 1 - 1) + (2 \cdot 2 - 1) + (2 \cdot 3 - 1) = 3^2$

Induction over the natural numbers

We can prove $\forall(n \mid 0 < n : P(n))$ as follows:

- First prove $P(0)$
- Then prove that for all $n \geq 0$, if $P(0), \cdots, P(n-1)$ hold, then so does $P(n)$

$$\forall(n : \mathbb{N} \mid 0 < n : P(0) \wedge P(1) \wedge \cdots \wedge P(n-1) \implies P(n))$$

- We do not really have to prove $P(n)$ in this way (suffices to know that in principle we can do so)
- The proofs of $P(0)$ and $\forall(n : \mathbb{N} \mid 0 < n : P(0) \wedge P(1) \wedge \cdots \wedge P(n-1) \implies P(n))$ are all we need to conclude that $P(n)$ holds for all natural numbers

Mathematical induction is formalised as a single axiom in the predicate calculus as follows, where $P : \mathbb{N} \longrightarrow \mathbb{B}$

Axiom (Mathematical Induction over $\mathbb{N}$)

$$\forall(n : \mathbb{N} \;|\!:\; \forall(i \mid 0 \leq i < n \;:\; P(i)) \implies P(n))$$
$$\implies \forall(n : \mathbb{N} \;|\!:\; P(n))$$

Theorem (Mathematical Induction over $\mathbb{N}$)

$$\forall(n : \mathbb{N} \;|\!:\; \forall(i \mid 0 \leq i < n \;:\; P(i)) \implies P(n))$$
$$\iff \forall(n : \mathbb{N} \;|\!:\; P(n))$$

Induction over the natural numbers

Theorem (Mathematical Induction over $\mathbb{N}$)

$$P(0) \ \wedge \ (\ \forall(n:\mathbb{N} \ |: \ \ \forall(i \ | \ 0 \leq i \leq n \ : \ P(i)\,) \implies P(n+1)\,)\,)$$
$$\implies \ \forall(n:\mathbb{N} \ |: \ P(n)\,)$$

- Conjunct $P(0)$ is called the base case of the mathematical induction
- $\forall(n:\mathbb{N} \ |: \ \ \forall(i \ | \ 0 \leq i \leq n \ : \ P(i)\,) \implies P(n+1)\,)$ is called the inductive case of the mathematical induction

Definition (Weak Mathematical Induction over $\mathbb{N}$)

$$P(0) \;\wedge\; \forall(n : \mathbb{N} \;|\!:\; P(n) \implies P(n+1)\,)$$
$$\implies \; \forall(n : \mathbb{N} \;|\!:\; P(n)\,)$$

- Conjunct $P(0)$ is called the base case of the mathematical induction

- $\forall(n : \mathbb{N} \;|\!:\; P(n) \implies P(n+1)\,)$ is called the inductive case of the weak mathematical induction

Theorem (Weak Mathematical Induction over $\mathbb{N}$)

$$P(0) \;\wedge\; \forall(n : \mathbb{N} \;|:\; P(n) \implies P(n+1)\,)$$
$$\iff \;\forall(n : \mathbb{N} \;|:\; P(n)\,)$$

- Proving $\forall(n : \mathbb{N} \;|:\; P(n) \implies P(n+1)\,)$ is often technically easier than proving $\forall(n : \mathbb{N} \;|:\; \forall(i \mid 0 \leq i \leq n \;:\; P(i)\,) \implies P(n+1)\,)$
- However sometimes we cannot prove $P(n) \implies P(n+1)$, while we can prove $\forall(i \mid 0 \leq i \leq n : P(i)) \implies P(n+1)$.

Induction over the natural numbers

- When proving $\forall(n : \mathbb{N} \mid: P(n))$ by induction, we often prove the base case and inductive case separately and then assert, in English, that $P(n)$ holds for all natural numbers n
- The proof of the inductive case is typically done by proving $\forall(i \mid 0 \le i \le n : P(i)) \implies P(n+1)$ for arbitrary $n \ge 0$
- Further, $\forall(i \mid 0 \le i \le n : P(i)) \implies P(n+1)$ is usually proved by assuming $\forall(i \mid 0 \le i \le n : P(i))$ and then proving $P(n+1)$

Example

We prove $P(n)$ for all natural numbers.

1. $P(n)$: $+(i \mid 1 \le i \le n : 2i - 1) = n^2$. (weak induction suffices)
2. $P(n)$: If $n \ge 1$, then n is a product of primes. Assume that 1 is a prime number (weak induction does not work).

Induction over the natural numbers

- Induction can be performed over any subset $n_0, n_0+1, n_0+2, \cdots$, of the integers

- The only difference in such a proof is the starting point and thus the base case

Theorem (Mathematical Induction over $\{n_0, n_0+1, \cdots\}$)

$$P(n_0) \wedge (\forall(n:\mathbb{N} \mid n_0 \leq n : \forall(i \mid n_0 \leq i \leq n : P(i)) \implies P(n+1)))$$
$$\implies \forall(n:\mathbb{N} \mid n_0 \leq n : P(n))$$

Theorem (Weak Mathematical Induction over $\{n_0, n_0+1, \cdots\}$)

$$P(n_0) \wedge \forall(n:\mathbb{N} \mid n_0 \leq n : P(n) \implies P(n+1))$$
$$\implies \forall(n:\mathbb{N} \mid n_0 \leq n : P(n))$$

Induction over the natural numbers

Example (Example of a proof by induction)

1. Prove $2n + 1 < 2^n$, for $n \geq 3$
2. Consider a currency consisting of 2-cent and 5-cent coins. Show that any amount above 3 cents can be represented using these coins.
3. Prove $P(n)$: $\exists(h, k \mid 0 \leq h \wedge 0 \leq k : 2h + 5k = n)$

Note that (3) is the formalisation of (2).

Inductive definition

Suppose, we want to define b^n for $b : \mathbb{Z}$ and $n : \mathbb{N}$

- $b^n = \ \cdot(i \mid 1 \leq i \leq n \ : \ b)$

- An alternative style:

$$\begin{cases} b^0 & = & 1 \\ b^{n+1} & = & b \cdot b^n \text{ (for } n \geq 0) \end{cases}$$

- Or,

$$\begin{cases} b^0 & = & 1 \\ b^{n} & = & b \cdot b^{n-1} \text{ (for } n \geq 1) \end{cases}$$

Inductive definition

Example

Prove by mathematical induction that for all natural numbers m and n, $b^{m+n} = b^m \cdot b^n$.

Problem

A model for the number of lobsters caught per year is based on the assumption that the number of lobsters caught in a year is the average of the number caught in the two previous years. At the beginning of the application of this model, $100,000$ *lobsters were caught in year 1 and* $300,000$ *were caught in year 2.*
Define inductively L_n*, where* L_n *is the number of lobsters caught in year n, under the assumption of this model and its initial conditions.*

- Base case: $L_1 = 100,000$ and $L_2 = 300,000$
- Inductive part: $L_n = \frac{L_{n-2}+L_{n-1}}{2}$

Inductive definition

Problem

- *A path is 2 metres wide and n metres long. It is to be paved using paving stones of size* $1m \times 2m$*. In how many ways can the paving be accomplished? Justify your answer.*
- *Consider the following game, played with a non-empty bag S of positive real numbers. Operation avg removes two elements of S (at random) and inserts two copies of the average of the two removed elements. The game terminates when all numbers in S are equal. Does the game always terminate?*

- Base case: $p_1 = 1$ and $p_2 = 2$
- Inductive part: $p_n = p_{n-1} + p_{n-2}$

Induction and well-founded sets

- We now generalise the notion of mathematical induction to deal with sets other than $\mathbb{N}$ and other relations
- For example, we can use mathematical induction to prove properties of binary trees with the relation "tree t' is a subtree of tree t".
- Let $\prec$ be a boolean function of two arguments of type U
- We want to determine the cases in which $\langle U, \prec \rangle$ admits induction (induction over $\langle U, \prec \rangle$ is sound)
- Not every pair $\langle U, \prec \rangle$ admits induction

We write the principle of mathematical induction over $\langle U, \prec \rangle$ as follows

Axiom (Mathematical induction over $\langle U, \prec \rangle$)

$$\forall(x \;|\!: \; P(x)\,)$$
$$\iff \; \forall(x \;|\!: \; \forall(y \mid y \prec x \; : \; P(y)\,) \implies P(x)\,)$$

- In the case $\langle U, \prec \rangle = \langle \mathbb{N}, < \rangle$ the above formulation reduces to the induction over $\mathbb{N}$
- We want to show that mathematical induction has two characterizations

Definition (Minimal element)

Element y is a minimal element of S if $y \in S$ and $\forall(x \mid x \prec y : x \notin S)$

Example

1. For $\langle \mathbb{N}, < \rangle$, the minimal element of any nonempty subset of $\mathbb{N}$ is its smallest element, in the usual sense.
2. Consider $\langle \mathbb{N}, \text{pdiv} \rangle$, where i pdiv j means "i is a divisor of j and $i < j$"
   - Then the subset $S = \{5, 15, 3, 20\}$ has two minimal elements, 5 and 3
3. Consider $\langle \mathbb{P}, \text{pdiv} \rangle$, where $\mathbb{P}$ is the set of prime numbers
   - All elements of $\langle \mathbb{P}, \text{pdiv} \rangle$ are minimal

Induction and well-founded sets

We use this notion of minimal element to define well foundedness

Definition (Well foundedness)

$\langle U, \prec \rangle$ is well founded if every nonempty subset of U has a minimal element, i.e.,

$$\forall(S \mid S \subseteq U : S \neq \emptyset \iff \exists(x \mid: x \in S \wedge \forall(y \mid y \prec x : y \notin S)))$$

Example

- $\langle \mathbb{N}, < \rangle$ is well founded
- $\langle \mathbb{Z}, < \rangle$ is not well founded

We now prove a remarkable fact: well foundedness of $\langle U, \prec \rangle$ and mathematical induction over $\langle U, \prec \rangle$ are equivalent

Theorem (Well-Foundness and Induction)

$\langle U, \prec \rangle$ is well founded iff it admits induction.

Proof.

The proof rests on the fact that for any subset S of U we can construct the expression $P(z) \iff z \notin S$, and for any boolean expression $P(z)$ we can construct the set $S = \{z | \neg P(z)\}$ ∎

$$S \neq \emptyset \iff \exists(x \mid: x \in S \wedge \forall(y \mid y \prec x : y \notin S))$$

$$\iff \quad \langle (\neg p \iff q) \iff (p \iff \neg q) \;\; \& \;\; (X \iff Y) \iff (\neg X \iff \neg Y) \;\; \& \;\; \text{Double negation} \rangle$$

$$S = \emptyset \iff \neg(\exists(x \mid: x \in S \wedge \forall(y \mid y \prec x : y \notin S)))$$

$$\iff \quad \langle \text{De Morgan} \;\; \& \;\; \text{Generalised De Morgan} \rangle$$

$$S = \emptyset \iff \forall(x \mid: x \notin S \vee \neg(\forall(y \mid y \prec x : y \notin S)))$$

$$\iff \quad \langle P(z) \iff z \notin S \text{ –replace occurrences of } S \rangle$$

$$\forall(x \mid: P(x)) \iff \forall(x \mid: P(x) \vee \neg(\forall(y \mid y \prec x : P(y))))$$

$$\iff \quad \langle \text{Law of implication} \rangle$$

$$\forall(x \mid: P(x)) \iff \forall(x \mid: \forall(y \mid y \prec x : P(y)) \implies P(x))$$

There is another characterization of well foundedness, in terms of the decreasing finite chain property

- Consider again $\langle U, \prec \rangle$, and define predicate DCF(x):
  DCF(x) : "every decreasing chain beginning with x is finite"

- We formalize the property of finite chain as follows:

Axiom (Finite chain property)

$$\forall(x \;|: \; \forall(y \;|\; y \prec x \;:\; DCF(y)\,) \implies DCF(x)\,)$$

Induction and well-founded sets

Definition

$\langle U, \prec \rangle$ is noetherian iff $\forall (x : U \;|{:}\; \mathrm{DCF}(x))$

Theorem

$\langle U, \prec \rangle$ is well founded iff $\langle U, \prec \rangle$ is noetherian

Theorem

If $\langle U, \prec \rangle$ admits induction, then $\prec$ if irreflexive, that is,
$\forall (x \mid x \in U : x \not\prec x)$

Theorem

If $\langle U, \prec \rangle$ admits induction, then
$\forall (x, y \mid x, y \in U : x \prec y \implies y \not\prec x)$

The correctness of loops

- We introduce a theorem concerning the while loop while B do S
- The proof of the theorem will show how correctness of a loop is inextricably intertwined with induction
- Following the textbook we write often a while loop using the syntax

$$\text{do } B \longrightarrow S \text{ od}$$

  where boolean expression B is called the guard and statement S is called the repetend

The correctness of loops

Example

$\{Q: \ \ 0 \leq n\}$

$i, p \ := \ 0, 0;$

$\{P: \ \ 0 \leq i \leq n \ \wedge \ p = i \cdot x\}$

$\text{do } i \neq n \longrightarrow i, p \ := \ i+1, p+x \text{ od}$

$\{R: \ \ p = n \cdot x\}$

- This loop execution requires exactly n iterations
- There is a loop invariant P (i.e., $0 \leq i \leq n \ \wedge \ p = i \cdot x$)

Theorem (Fundamental invariance theorem)

Suppose

- $\{P \ \wedge \ B\}\ S\ \{P\}$ *holds, and*
- $\{P\}$ do $B \longrightarrow S$ od $\{\text{true}\}$ *(i.e., execution of the loop begun in a state in which P is true terminates)*

Then $\{P\}$ do $B \longrightarrow S$ od $\{P \ \wedge \ \neg B\}$ *holds.*

Proof.

Proof by induction on the number of iterations. ∎

Example

Prove the following Hoare triple

$$\{P: \ 0 \leq i \leq n \ \wedge \ p = i \cdot x\}$$
$$\text{do } B: \ \ i \neq n \longrightarrow i, p \ := \ i+1, p+x \text{ od}$$
$$\{P \ \wedge \ i = n\}$$

Main Proof Steps:

- We prove the first hypothesis of the theorem

$$\{P \ \wedge \ B\} \ i, p \ := \ i+1, p+x \ \{P\}$$

- We prove the second hypothesis of the theorem (Execution of the loop terminates)

Then we conclude that the above Hoare triple holds

$\{P\}$
do $B \longrightarrow S$ od
$\{R\}$

Checklist for proving loop correct

1. P is true before execution of the loop
2. P is a loop invariant: $\{P \wedge B\}\ S\ \{P\}$
3. Execution of the loop terminates
4. R holds upon termination: $P \wedge \neg B \implies R$

Example

Use the checklist to prove that the annotation in this program is correct.

$\{0 \leq n\}$

$i, p \ := \ 0, 0;$

$\{\text{invariant } P : 0 \leq i \leq n \ \wedge \ p = i \cdot x\}$

$\text{do } i \neq n \longrightarrow i, p \ := \ i + 1, p + x \text{ od}$

$\{R : \ \ p = n \cdot x\}$

The correctness of loops

Problem

Use the checklist to prove that the annotation in this program is correct.

$$\{Q: \;\; b \geq 0 \;\wedge\; c > 0\}$$
$$q, r \;:=\; 0, b;$$
$$\{invariant\ P : b = q \cdot c + r \;\wedge\; 0 \leq r\}$$
$$\text{do } r \geq c \longrightarrow q, r \;:=\; q + 1, r - c \text{ od}$$
$$\{R: \;\; b = q \cdot c + r \;\wedge\; 0 \leq r < c\}$$

The correctness of loops

Consider the following program

$$
\begin{array}{l}
\{0 \leq i = I\} \\
q, r \;:=\; 0, b; \\
\{\text{invariant } P : 0 \leq i\} \\
\text{do}\, 0 \neq i \longrightarrow \quad \text{if} \quad \text{true} \longrightarrow i \;:=\; i - 1 \\
\qquad\qquad\qquad\quad [] \quad i \neq 1 \longrightarrow i \;:=\; i - 2 \\
\qquad\qquad\qquad\quad\; \text{fi} \\
\{R : \;\; i = 0\}
\end{array}
$$

- It is readily seen that invariant P is initially true, that the repetend maintains P, and that $P \;\wedge\; \neg(0 \neq i) \implies R$
- We can argue that loop terminates after at most I iterations
- More generally, we can prove the following theorem

The correctness of loops

Theorem

To prove that

$\{$*invariant:* $P\}$

$\{$*bound function:* $T\}$

do $B \longrightarrow S$ od

terminates, it suffices to find a bound function T*, i.e., an integer expression* T *that is an upper bound on the number of iterations still to be performed. Thus, bound function* T *satisfies:*

1. T *decreases at each iteration: that is, for* v *a fresh variable,* $\{P \ \wedge \ B\}\ v \ := \ T; S\ \{T < v\}$
2. *As long as there is another iteration to perform,* $T > 0 : P \ \wedge \ B \implies T > O.$

Proof.

We prove the theorem by induction on the initial value of T ∎

Remarks:

- This method of proof does not work with all loops
- Termination proofs might use other well-founded sets
- Examples will be presented in the tutorial

Example (Factorial)

Consider the following program

Pr: $\quad i := 1;\ factorial := 1;$

$\quad\quad$ while $i < n$ do

$\quad\quad$ begin $i := i + 1;\ factorial := factorial * i$ end

$\quad\quad$ od.

Let $Q = (factorial = i! \wedge i \leq n)$.

We can show (using rules for assignment) that

$\{(factorial = i! \wedge i \leq n) \wedge i < n\}$

$i := i + 1;\ factorial := factorial * i$

$\{factorial = i! \wedge i \leq n\}$,

so Q is the loop invariant.

Since $\neg(x < n) \wedge Q \iff factorial = n!$, we have

$$\{\text{true}\}\ Pr\ \{factorial = n!\}$$

Example (Factorial-continued)

- Let solve:
  $\{\ ?\ \}$
  $i := i+1;\ factorial := factorial * i$
  $\{factorial = i! \wedge i \leq n\}$.
- From the definition of sequential composition of two assignment statements we have:
  $\{(factorial = i! \wedge i \leq n)[factorial := factorial * i][i := i+1]\}$
  $i := i+1;\ factorial := factorial * i$
  $\{factorial = i! \wedge i \leq n\}$.
- Hence:
  $(factorial = i! \wedge i \leq n)[factorial := factorial * i][i := i+1]$
  $\iff (factorial * i = i! \wedge i \leq n)[i := i+1] \iff$
  $factorial * (i+1) = (i+1)! \wedge i+1 \leq n \iff$
  $factorial * (i+1) = i! * (i+1) \wedge i < n \iff$
  $factorial = i! \wedge i < n \iff (factorial = i! \wedge i \leq n) \wedge i < n$.
- Which means $\{\ ?\ \} = \{(factorial = i! \wedge i \leq n) \wedge i < n\}$.